

## **PERSONNEL SECURITY AND SUITABILITY PROGRAM**

---

### **I. Purpose**

This directive establishes Department of Homeland Security (DHS) policy regarding the Department-wide Personnel Security Program.

### **II. Scope**

This directive applies to DHS Organizational Elements, DHS employees, and detailed personnel providing support to DHS activities and operations. This directive defines the minimum standards, but does not prohibit any Organizational Element from exceeding the requirements based on mission or potential for adverse impact on National Security. Any requests to lower these minimum standards must be approved in advance by the DHS Office of Security.

### **III. Authorities**

- A. Executive Order 10450, "Security Requirements for Government Employees," dated April 27, 1953, as amended.
- B. Executive Order 10577, "Amending the Civil Service Rules and Authorizing a New Appointment System for the Competitive Service," dated November 22, 1954, as amended.
- C. Executive Order 12958, "Classified National Security Information," dated April 17, 1995, as amended.
- D. Executive Order 12968, "Access to Classified Information," dated August 2, 1995, as amended.
- E. Title 5, Code of Federal Regulations, Part 731, "Suitability."
- F. Title 5, Code of Federal Regulations, Part 732, "National Security Positions."
- G. Title 5, Code of Federal Regulations, Part 736, "Personnel Investigations."
- H. Title 32, Code of Federal Regulations, Part 147, "Adjudicative Guidelines"

for Determining Eligibility for Access to Classified Information.”

I. Title 5, United States Code, Section 552, “The Freedom of Information Act,” as amended.

J. Title 5, United States Code, Section 552(a), “The Privacy Act of 1974,” as amended.

K. Office of Management and Budget Circular No. A-130, “Security of Federal Automated Information Resources.”

L. Office of Personnel Management, Investigations Service, Investigator’s Handbook, February 1999.

M. Director of Central Intelligence Directive (DCID) 6/4, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information (SCI),” July 2, 1998.

N. DHS Management Directive 0010.1, “Management Directives System and DHS Announcements.”

O. DHS-delegation 8001, “Delegation to the Chief, Office of Security, for Security Clearances of DHS Personnel.”

P. Designation to the Chief Security Officer to act as “Senior Agency Official,” dated March 3, 2004.

## IV. Definitions

A. **Access**: A determination that an employee requires access to a particular level of classified information in order to perform or assist in a lawful and authorized governmental function.

B. **Access National Agency Check and Inquiry (ANACI)**: Consists of a National Agency Check (NAC), employment checks, education checks, residence checks, reference checks, and law enforcement agency checks.

C. **Adjudication**: Evaluation of pertinent data contained in a background investigation, and/or any other available relevant reports, to determine whether an individual is eligible for access to classified information and for Federal employment.

D. **Background Investigation (BI)**: Consists of a National Agency Check (NAC), personal interviews with the individual and other sources, credit checks, law enforcement agency checks, residences checks, and employment checks.

E. **CONFIDENTIAL information:** Information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security of the United States.

F. **Employee:** A person other than the President and Vice President, employed by, detailed, or assigned to an agency, including members of the Armed Forces; other categories of persons who act for or on behalf of an agency, as determined by the appropriate agency head.

G. **Employment Position Sensitivity Categories.** Defined by the Office of Personnel Management.

1. **Non-Sensitive/Low Risk:** Non-Sensitive/Low Risk positions have the potential for limited impact on the integrity and efficiency of the service. These positions involve duties and responsibilities of limited relation to an agency or program mission.
2. **Moderate Risk:** Moderate Risk positions have the potential for moderate to serious impact on the integrity and efficiency of the service. These positions involve duties that considerably important to the agency or program mission with significant program responsibility or delivery of service.
3. **High Risk:** High-Risk positions have the potential for exceptionally serious impact on the integrity and efficiency of the service. These positions involve duties that are especially critical to the agency or program mission with a broad scope of responsibility and authority.
4. **Non-Critical Sensitive:** Non-Critical Sensitive positions have the potential for serious damage to the national security. These positions involve either access to SECRET or CONFIDENTIAL national security information materials, or duties that may adversely affect, directly or indirectly, the national security operations of the Department.
5. **Critical Sensitive:** Critical Sensitive positions have the potential for exceptionally grave damage to the national security. These positions may include access up to, and including, TOP SECRET national security information or materials; or other positions related to national security, regardless of duties, that require the same degree of trust.
6. **Special Sensitive:** Special Sensitive positions include any position designated at a level higher than Critical Sensitive that complement E.O. 10450 and E.O. 12968 (such as Director of Central Intelligence Directive 6/4 that sets investigative requirements and access to Sensitive Compartmented Information and other intelligence-related Special

Sensitive information).

- H. **Minimum Background Investigation (MBI)**: Consists of a National Agency Check (NAC), personal interview with the individual, reference checks, credit checks, law enforcement agency checks, residence checks, and employment checks. Other than the personal interview, there are no source interviews conducted during this investigation.
- I. **National Agency Check (NAC)**: Consists of records searches in the Office of Personnel Management (OPM) Security/Suitability Investigations Index (SII); FBI Identification Division/Headquarters investigation files; FBI National Criminal History Fingerprint File; Defense Clearance and Investigations Index (DCII); and other sources, as necessary, to cover specific areas of a subject's background.
- J. **National Agency Check and Inquiries (NACI)**: Consists of a NAC, employment checks, education checks, law enforcement agency checks, and personal reference checks.
- K. **National Crime Information Center (NCIC) Check**: Consists of a check of the computerized index of criminal justice information (e.g., criminal record history information, fugitives, stolen properties, missing persons).
- L. **National Security Positions**: Positions defined under Executive Orders 10450 and 12968 that involve activities of the U.S. Government concerned with the protection of the nation from foreign aggression or espionage. These include positions involved with developing defense plans or policies; intelligence or counterintelligence activities; foreign relations, and related activities concerned with preserving the military strength of the United States; and positions that require regular use of, or access to, classified information.
- M. **Need-to-Know**: A determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.
- N. **Organizational Element**: As used in this Directive, the term DHS Organizational Element (OE) shall have the meaning as defined in DHS MD 0010.1, "Management Directives System and DHS Announcements."
- O. **Public Trust Positions**: Positions defined under 5 CFR 731 that may involve policy making, major program responsibility, public safety and health, law enforcement duties, fiduciary responsibilities, or other duties demanding a significant degree of public trust; positions involving access to, or operation of, or control of financial records, with a significant risk for causing damage or realizing personal gain

P. **SECRET information**: Information, the unauthorized disclosure of which could reasonably be expected to cause serious damage to the national security of the United States.

Q. **Sensitive Information**: Any information, the loss, misuse, unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an act of Congress to be kept secret in the interest of national defense or foreign policy.

R. **Sensitive Compartmented Information (SCI)**: Classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling exclusively within formal access control systems established by the Director of Central Intelligence.

S. **Single Scope Background Investigation (SSBI)**: Consists of a National Agency Check (NAC)' a spouse or cohabitant NAC' a personal Subject Interview' and citizenship, education, employment, residence, law enforcement, and record searches covering the most recent ten (10) years of an individual's life, or since his or her 18th birthday, whichever is shorter.

T. **Suitability**: A determination based on an individual's character or conduct that may have an impact on the integrity or efficiency of their employment. Determinations made under this category are distinct from determinations of eligibility for assignment to, or retention in, sensitive national security positions.

U. **TOP SECRET information**: Information, the unauthorized disclosure of which could reasonably be expected to cause exceptionally grave damage to the national security of the United States.

## V. Responsibility

A. The Chief of Personnel Security Division, under the direction of the Chief Security Officer (CSO), has responsibility for oversight of the DHS Personnel Security Program, to include issuing, implementing, and compliance with policies and procedures.

B. All DHS Organizational Elements having a personnel security and suitability program are responsible for implementing and complying with the minimum standards required by this Management Directive. This Directive does not prohibit any Organizational Element from exceeding the requirements based on mission needs or the potential for an adverse impact on National Security.

However no Organizational Element may reduce the standards/requirements without prior approval of the Chief Security Officer.

## **VI. Policy & Procedures**

### **A. Policy.**

1. All positions within DHS shall be designated using the OPM Position Sensitivity Designation Guidance.
2. All DHS employees will be investigated commensurate with the position sensitivity as described in the OPM Position Sensitivity Designation Guidance. Investigations may be completed post-appointment/employment subject to the requirements outlined below.

### **B. Procedures.**

#### **1. Investigative Standard.**

- a. The investigation will be commensurate with the position sensitivity as described in the OPM Position Sensitivity Designation Guidance. Positions may be designated either as public trust positions or national security positions. Suitability is a consideration for every position.
- b. The minimum investigative standard will be the National Agency Check and Inquiries (NACI).
- c. Additional investigations may be required depending on the position sensitivity and/or access to classified information. Additional investigations include Minimum Background Investigation (MBI), Background Investigation (BI), and Single Scope Background Investigation (SSBI). (See Section IV, Definitions.)
- d. The minimum investigative standard for SECRET will be an MBI. The minimum investigative standard for TOP SECRET/SCI will be an SSBI.
- e. Employees who became DHS employees upon the creation of the Department, and whose investigation is less than the minimum standard, are considered as having met the requirement. Additional investigation may be required if the position sensitivity or the security clearance level is raised. Additional investigations also will be conducted as a result of the periodic re-investigation requirement.

2. **Pre-Appointment/Employment Investigations.**

a. For Public Trust Positions, the investigation may be completed post-appointment/employment for entry-on-duty purposes.

b. For National Security Positions, the investigation may be completed post-appointment/employment, provided that the following requirements are met:

(1) For positions designated Non-Critical Sensitive, investigations may be completed post appointment following favorable review of the Standard Form (SF) 86 and pre-employment checks.

(2) For positions designated Critical Sensitive, investigations may be completed post appointment/employment provided that:

(a) The SF 86 is completed and the required investigation has been initiated (if applicable).

(b) Check of the Security/Suitability Investigations Index (SII) at OPM and Defense Clearance and Investigations Index (DCII) at Defense Security Service have been completed (if applicable). If a recent investigation exists (within the previous five (5) years) the employing agency must obtain/review before entry on duty approval is granted.

(c) Fingerprint check results or NCIC results have been received.

(d) Credit check results have been received.

(e) All of the above checks must be favorable. If derogatory information exists, the investigation must be completed and favorably adjudicated prior to entry on duty.

(3) There is no waiver for Special Sensitive positions.

3. **Break in Service.** If a person who requires access has been retired or separated from U.S. Government employment for less than two years and is the subject of an investigation that is otherwise current (within

the past five (5) years), the agency may grant access following, at a minimum, a review of an updated SF 86 and applicable records. A reinvestigation is not required unless the review indicates the person may no longer satisfy the standards of Executive Order 12968.

4. **Temporary Access.** In accordance with Section 2.1(b)(3) of Executive Order 12968, temporary eligibility for access to classified information may be granted when there is a temporary need, such as one-time participation in a classified project, when investigative standards have been satisfied. In such cases, the expiration of this temporary access is identified by a fixed date or event, and access to classified information shall be limited to that related to the particular project or assignment.

5. **Interim Access.**

a. Interim access to SECRET classified information may be granted when there is an intention to grant a final security clearance once the pending background investigation is completed and favorably adjudicated. At a minimum, eligibility requires completion of the SF 86, including any applicable supporting documentation, favorable review of the form by the appropriate adjudicating authority, NCIC check, credit check, and fingerprint submission.

b. Interim TOP SECRET access will not be granted. Employees who have transitioned to DHS with an Interim TOP SECRET access are considered as having met the requirement. On an expedited basis, DHS Headquarters Personnel Security Division will work with the Organizational Elements to convert their employees' Interim TOP SECRET access to Final TOP SECRET status. Any requests for waivers to this policy must be approved in advance by the Chief Security Officer, Office of Security.

6. **Position Sensitivity Designation.** The supervising official with sufficient knowledge of duty assignments is responsible for assigning position sensitivity designations. Designations will be subject to final approval by the Organizational Element's respective Personnel Security Office. The DHS Office of Security retains the position sensitivity designation authority for:

a. All presidential appointees in the Department requiring confirmation by the Senate, to the extent of the Department's authority with respect to these officials;

b. Under Secretaries and their first deputies;



c. Organizational Element personnel security officers and any official with delegated authority to grant security clearances.

7. **Forms**. All employees are required to complete either the Standard Form (SF) 86 "Questionnaire for National Security Positions" or the Standard Form 85P "Questionnaire for Public Trust Positions," depending on position sensitivity designation.

8. **Access to Classified Information**.

a. Eligibility for access to classified information shall be granted in accordance with Executive Order 12968, as amended. Access will not be granted unless the individual has:

(1) Undergone the requisite background investigation required for the level of access;

(2) Been briefed regarding the responsibilities associated with access to classified information;

(3) Signed a Classified Information Non-Disclosure Agreement (SF 312);

(4) A "need-to-know" in order to do their job.

b. All employees will be adjudicated under the Adjudicative Standards set forth in 32 CFR 147, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information," to determine their eligibility for access to classified information.

c. All employees eligible for SCI access will be adjudicated under the Adjudicative Standards set forth in DCID 6/4, Annex C.

9. **Suitability**. Suitability is a consideration for every position. Suitability determinations will be made in accordance with 5 CFR 731, section 202.

10. **Reinvestigations**. An SSBI-PR will be conducted every five (5) years for TOP SECRET and SCI eligibility. An MBI will be conducted every ten (10) years for security and suitability purposes on all other employees to include employees who were grandfathered under legacy investigative requirements.

11. **Reciprocity**. Investigations conducted in accordance with Executive Order 12968 will be accepted by DHS without re-adjudication, unless there exists substantial information indicating an employee may not

satisfy the Executive Order 12968 standards. However, a new SF 86 is required. Further investigation will only be conducted to meet required reinvestigation or security clearance revalidation requirements, or if derogatory information exists.

12. **Eligibility Determinations**. Eligibility determinations will be made in accordance with 32 CFR 147, "Adjudicative Guidelines for Determining Eligibility for Access to Classified Information." These Guidelines apply to all individuals being considered for initial or continued eligibility for access to classified information and are used in all security clearance determinations. In the event an individual fails or ceases to meet the standards for a security clearance, he/she will be provided with the appropriate due process in accordance with the applicable law, rule, and/or regulation.

13. **Waiver Requests**. Any request for exemptions to the above requirements must be submitted, in writing, to the Office of Security, Chief Security Officer. Waiver requests should include a justification and will be considered on a case-by-case basis.

## VII. Questions

Questions regarding this Directive should be addressed to the Office of Security, Chief of the Personnel Security Division.